Strategic Foresight and the EU Cyber Threat Landscape in 2025: a Workshop Report

Weber, Valentin; Toriser, Victoria Cygne Lara

Veröffentlichungsversion / Published Version
Kurzbericht / abridged report

DGAP REPORT

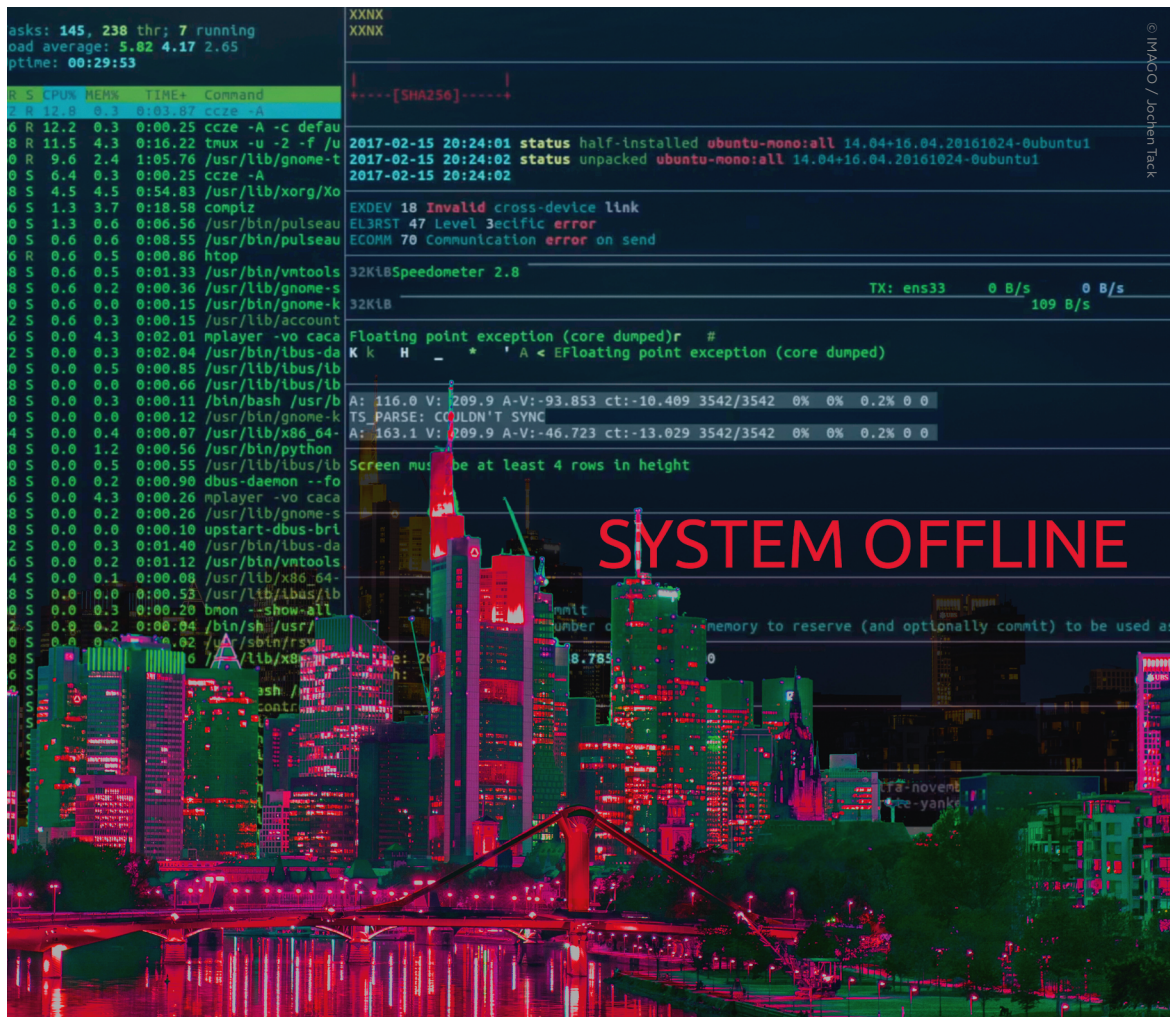# Strategic Foresight and the EU Cyber Threat Landscape in 2025

A Workshop Report

Valentin Weber
Research Fellow, Technology and Global Affairs Program, German Council on Foreign Relations (DGAP)

Victoria Cygne Lara Toriser
Consultant for Strategic Foresight and Strategic Management, REPUCO Management Consultancy

INTRODUCTION

The member states of the European Union (EU) face an unprecedented challenge arising from cybercrime perpetrated by both non-state actors and well-resourced state actors. Europe's industry suffers from industrial espionage and its foreign ministries from advanced persistent threats. In 2020, Germany even experienced what was described by some as the first death resulting from cyber means when a ransomware attack caused the unavailability of systems at a hospital. A patient was consequently turned away from Düsseldorf University Hospital and transferred to a different hospital, leading to her death.

To look beyond the present and provide an outlook into the future cyber threat landscape, the German Council on Foreign Relations (DGAP) hosted several workshops in September 2021 with experts from industry, academia, European ministries, and international organizations. In addition to contemplating how a future cyber threat landscape might look, participants envisioned strategies and mechanisms that the EU could deploy to overcome the various challenges that lie ahead.

These workshops employed scenario planning, a technique widely used by think tanks, the intelligence community, and the military. Workshop participants engaged in what the RAND Corporation's Herman Kahn once dubbed "ersatz experience," a term designating thought experiments that draw on an imagined future – rather than on past experience, which is a notoriously bad predictor of future events. In doing so, they crafted two plausible future scenarios for European policy-makers that are characterized by different levels of disruption.

STRATEGIC FORESIGHT

The aim of any foresight project is to enable decision-makers to find effective and accurate strategies to reach a desired future or to successfully deal with crises once they occur. The first step is always to define the object of investigation in terms of theme, context, and time. This environmental analysis is used to develop a system picture. Then, scenarios can be developed that reflect different futures for the object of investigation.

The object of investigation in our workshops was the development of the cyber threat environment of the EU in the next five years. Therefore, our first task was to identify themes/fields of influence – including state actors, technological developments, etc. – that will affect the development of the cyber and hybrid threat environment in that time. Next, we had to define the factors that influence each of these themes/fields of influence. An influencing factor is a measurable or describable entity whose manifestation can change over time. Using intuitive methods to brainstorm ideas, the workshop participants were asked to first list as many factors as possible and then evaluate them based on their level of relevance and uncertainty (uncertainty analysis). The most relevant and interconnected fac-

FIGURE 1: THE STRATEGIC FORESIGHT PROCESS (SCENARIO AND STRATEGY DEVELOPMENT)

Environmental analysis

Elicitation of key factors

Derivation of future projections

Scenario development

Consequence analysis

Strategy development

Strategy evaluation

Source: Authors' own compilation

tors were deemed key factors and, therefore, selected for further processing.

Explorative scenarios were constructed based on these key factors (e.g., malware, cybercrime, advanced persistent threats) and how they are likely to develop in the future. The scenario team's next task was to identify up to five possible projections of each of the key factors. After several future projections were determined for the key factors, scenarios could then be formed from them.

In the following step, workshop participants were divided into two groups. Group 1 focused on imagining a disruptive cyber threat scenario and Group 2 a non-disruptive cyber threat scenario. The two teams picked projections fitting to their scenario title. In this way, they created one scenario per group out of a combination of several projections of key factors.

After having created two scenarios, the next task was to think of effective strategies for addressing each one – also identifying the strategy best suited to react to both.

The strategies for each of the scenarios need to be sufficiently complex and draw from a multitude of strategic options. Hence, the workshop participants had to analyze the fields of action (e.g., security and defense policy, diplomacy) for Europe in regard to the future cyber threat environment and identify strategic options within those fields of action (e.g., confidence-building measures, establishing contact points between governments). Subsequently, they developed strategies by choosing differing sets of strategic options for each of the strategies while keeping in mind that the objective is to find a strategy that potentially suits both scenarios.

The core questions that guided the strategy development process were:

- How must the respective strategy be designed (composed of action options) to effectively counter the risks and threats of the assigned scenario and, at the same time, exploit and seize the opportunities of the scenario as much as possible?

- Which sets of strategic options should be selected to develop effective strategies for each of the scenarios?

The final step for the workshop participants was to evaluate the strategies to identify the most robust one that has the potential to be effective in case either of the scenarios materializes. Usually, this would be followed by the deduction of recommendations for action for both operative and political decision-makers. By choosing and implementing

FIGURE 2: STRATEGY DEVELOPMENT AND EVALUATION
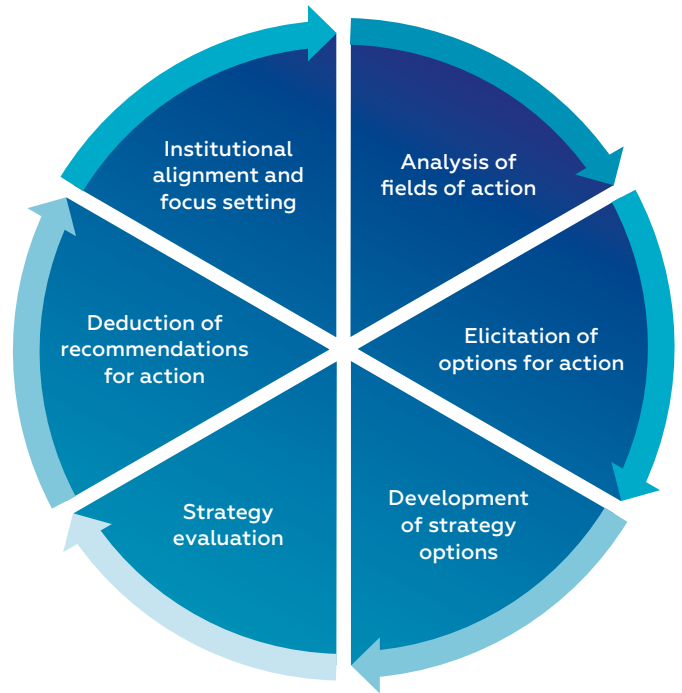
Source: Authors' own compilation

a strategy, new focus points for future action are set and policies derived. The steps illustrated in Figure 2 should be repeated in the framework of future foresight workshops to account for changing circumstances in the cyber threat environment.

SCENARIO 1: A DISRUPTIVE CYBER THREAT LANDSCAPE

A disruptive cyber threat landscape is defined as a landscape that is considerably more disruptive in the future than today in terms of magnitude, scope, and duration.

This scenario expects an increasing automation of malware that is inserted through supply chains. In such an environment, artificial intelligence (AI) gives the offense an advantage, which makes defense even more difficult than it already is. More and more, both offense and defense will rely on near-real-time AI to attack and defend. Humans are increasingly being taken out of the loop. This brings up questions of oversight over decisions taken by algorithms and how it is used. To give an example, who is responsible if damages happen during cyber operations in which humans are not making the decisions?

FIGURE 3: KEY FACTORS IN THE CYBER THREAT LANDSCAPE
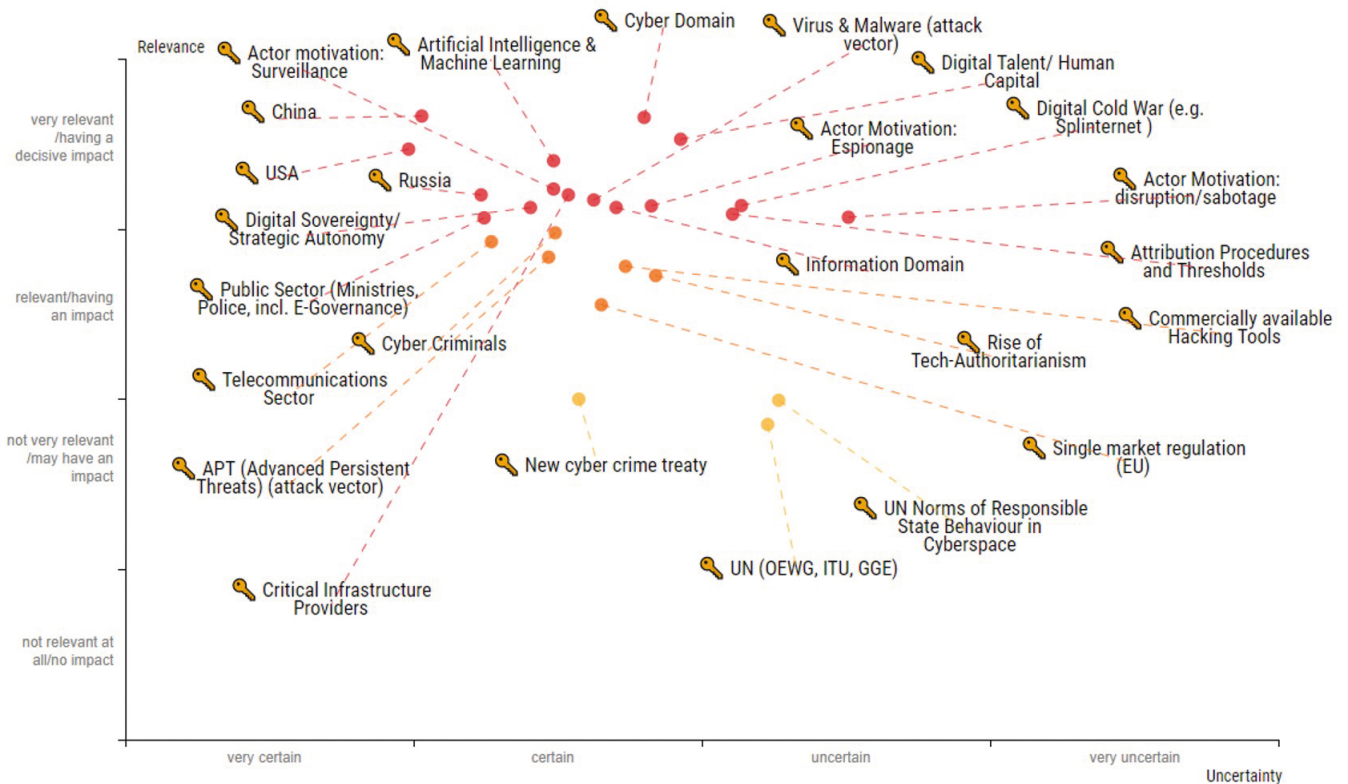
Source: Foresight Strategy Cockpit[1] and DGAP workshop analysis

At the same time, this scenario expects the scope of attacks against actors who hold offensive tools to increase considerably. The acquisition of advanced offensive tools makes the environment even more unstable. Although cyber espionage operations become bolder, no norms could be agreed upon in this respect.

Critically, cyber criminals enable state cyber operations, leading to unintended escalation. The use of cyber mercenaries increases, especially if states cannot agree on a state actor that is responsible for non-state actor operations emanating from their territories. Workshop participants expect high grade attacks to still rely on state capabilities even though they may be used by non-state actors. Organized crime groups also start working with terrorists, elevating their potential to cause harm.

In a future in which digital natives enter the cybercrime market, most crime relies on digital infrastructure. Regulation of the cybercrime market is very difficult. Because the market for cyber weapons is developed by too many actors, major law enforcement agencies are unable to buy them up. Also, many offensive tools are just not available for purchase. The combination makes it very difficult to dry up this market.

Regarding international negotiations in a disruptive environment, the experts are almost certain that a new cybercrime treaty is concluded. Yet they remain unsure about its content. A new round of discussions by the United Nations Group of Governmental Experts (UNGGE) is unlikely to occur. Instead, more and more cyber security discussions are held within the UN's Open-ended Working Group (OEWG).

---

1   To develop the scenarios and strategies, workshop participants used the Foresight Strategy Cockpit (FSC), a web-based tool that allows companies and organizations to manage a holistic foresight process ranging from trend analysis and risk analysis to scenario and strategy development. Further information can be found at https://www.4strat.com/strategy-foresight-service/foresight-strategy-cockpit/ (accessed November 8, 2021).

SCENARIO 2: A NON-DISRUPTIVE CYBER THREAT LANDSCAPE

The workshop participants who engaged in this second scenario determined that a non-disruptive future cyber threat landscape still includes regular high profile cyber operations that receive widespread attention. However, countries and non-state actors refrain from bluntly crossing red lines in cyberspace, such as attacking nuclear command and control systems. Some geopolitical tensions related to cyber security may be mitigated through open standards, for example in the telecommunications sector.

The participants expect the continuing use of phishing to activate viruses and malware. "Interaction" remains the most pertinent vector for delivering malware. Due to the fact that funding for AI is funneled into both offensive and defensive technologies, neither the offense nor defense is provided a clear advantage by AI and machine learning.

In the information domain, both information and disinformation are used as part of hybrid activities that fall within the broader strategy of malicious actors. This intensification of hybrid activities increases the fog of war for the defense.

The public sector – including ministries, police, and e-governance – grows to be even more tech dependent, making it a valuable target. Few sectors face a more challenging threat environment than the public sector. Recent ransomware and sophisticated supply chain attacks, for example the ransomware attack on the Health Service Executive of Ireland in May 2021, remain a valuable reminder of that. In this non-disruptive cyber future, though, the public sector does not enhance its cyber security measures. This leads to considerable vulnerabilities in EU member states.

Workshop participants see incompatible strategic cultures within the EU leading to prolonged struggles over digital sovereignty – with alliances within the EU changing according to interests and opportunities. At the same time, the United States is likely to remain a major cyber power that continues defending forward with little restraint. Meanwhile, China seeks to amass more power through cyber diplomacy and strategic investments funneled through its Digital Silk Road. Russia tests the threshold for cyber conflict with aggressive campaigns, but it does not cross major red lines in cyberspace.

EU STRATEGY 1: TAKING ON A DISRUPTIVE FUTURE CYBER THREAT LANDSCAPE

In a highly disruptive environment, the European Union should focus on three main things:

The EU must assume a values-based de-escalatory cyber posture.

Unlike the United States, which has taken a defending forward cyber posture, the European Union should take on a more defensive posture. Workshop participants agreed that, in a future in which the environment is highly unstable, engaging in highly offensive operations would be non-beneficial to the EU.

The EU should take a values-based approach that places fundamental human rights at the core of its cyber foreign policy. Its stance should be that it cannot exclude human rights considerations from its decisions on cyber risk, for example its assessment of equipment that goes into critical infrastructure.

At home, the EU needs to continue to build resilience. It ought to encourage a change in the behavior of consumers by nudging them toward secure behavior through security by design, which is intuitive and does not require IT skills.

EU member states need to be bolder in UN negotiations.

In upcoming negotiations in the UN's OEWG, as well as in cybercrime treaty negotiations, EU member states should also pursue a values-based cyber foreign policy.

EU member states should prevent terms that focus on the manipulation/security of information from gaining traction in UN discussions. In a disruptive cyber threat landscape, the EU needs to make sure that whenever *discussions* occur at the international level, they result in a clear roadmap to *implementing* any agreement with consequences and verifiable action. As one of the workshop participants noted: "Do we want to negotiate a [cybercrime] treaty for five years if it won't be implemented?"

EU member states need to make their statements on how international law applies to cyberspace more coherent. In an unstable future, they also need to abandon their reticence to invoke international law. In addition, EU member states should push for provisions on the role of states to monitor and be accountable to the actions of non-state actors that operate from their territory.

Sanctions are unavoidable but should not be prioritized.

The participating experts agreed that sanctions, although necessary, should not be prioritized in the EU's strategy.

Targeted sanctions against individuals, which include travel bans and asset freezes, represent the status quo. This approach currently appears to be quite ineffective and might be even more so in a disruptive environment.

Sector-based sanctions might not be a satisfying solution either. Those sanctions would affect sectors related to an attack. For example, the EU could prohibit some IT equipment coming from Russia or China from entering the EU market. Such an approach may prove toothless in regard to Russia because so little equipment is of Russian provenance. It would also be difficult to implement with regard to China since the EU relies on technology from China and could not easily find a substitute supplier for equipment in the short term.

EU STRATEGY 2: TAKING ON A NON-DISRUPTIVE FUTURE CYBER THREAT LANDSCAPE

In a non-disruptive cyber and hybrid threat landscape, the European Union should focus on three main things:

The EU must pursue strategic autonomy and some offense in its cyber posture.

Although the EU should closely coordinate with the United States, it should pursue long-term strategic autonomy and the ability to pursue independent actions in the technological realm. With regard to Russia, EU member states should keep their distance while maintaining diplomatic dialogue. The same approach counts for China. Due to the non-disruptive nature of the threat environment, it is less likely that the EU will develop coherence in responding to external threats. Workshop participants believe that while some member states could engage in a more active way in responding to cyber threats, others could take a posture focused on defense. Taking an active posture in a non-disruptive environment may lead to less escalation and instability than in a disruptive environment.

The EU should increase its use of sanctions and market leverage.

Workshop participants in the non-disruptive group had different views on the effectiveness of sanctions from those in the disruptive group, resulting in opposing views on their use. In this non-disruptive scenario, the EU should expand its cyber diplomacy toolbox and define red lines for hostile cyber operations. The use of sanctions should be extended from current targeted sanctions against individuals and entities to sector-based sanctions. The EU should also consider a broader use of its market size as leverage against hostile states. Imposing sanctions and publicly blaming hostile actors as a response to cyberattacks will require considerable investment in the attribution capabilities of EU member states.

The EU should invest in cyber attribution and multi-domain situational awareness capability.

Due to the multi-domain activities of malicious actors, the EU should focus its ambitions toward the use of AI on enhancing situational awareness in the information manipulation space and attribution capabilities in the cyber domain. This effort aims to detect anomalies, indicators, and new trends and developments to identify hybrid activities and threats. This should help with the analysis of emerging action patterns of hostile actors.

WHY THE EU SHOULD PURSUE STRATEGY 1

Having crafted multiple scenarios and strategies, workshop participants found that a disruptive future cyber threat landscape (Scenario 1) is more likely than a non-disruptive one (Scenario 2). The participating experts also agreed that Strategy 1, which was designed to face a disruptive cyber threat environment, could simultaneously cope well with a non-disruptive cyber threat landscape. Moreover, they determined that, when comparing a disruptive and non-disruptive scenario, it is best to prepare for the worst. Therefore, Strategy 2 was perceived to be less suited to a disruptive cyber future because it recommends that some EU states take on a more offensive cyber posture, which would likely be escalatory in such a landscape. Consequently, workshop participants picked Strategy 1 for EU member states to pursue.

CONCLUSION

The primary goal of these workshops was not to produce a comprehensive and extensive report. Rather, they aimed to provide an initial assessment of potential future cyber scenarios and to create some "ersatz experience" for EU policy-makers. We hope that this written output will give some impetus to conduct further foresight exercises in a cyber-security context and that these methods will be further integrated into political decision-making processes within the EU.

DGAP

Advancing foreign policy. Since 1955.

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).